Pell方程式の理論の非Abel拡大への応用 (代数的整数論研究会報告集)

AUTHOR(S):

黒田, 成信

CITATION:

黒田, 成信. Pell方程式の理論の非Abel拡大への応用 (代数的整数論研究会報告集). 数理解析研究所講究録 1968, 41(2): 1-9

ISSUE DATE:

1968-06

URL:

http://hdl.handle.net/2433/107650

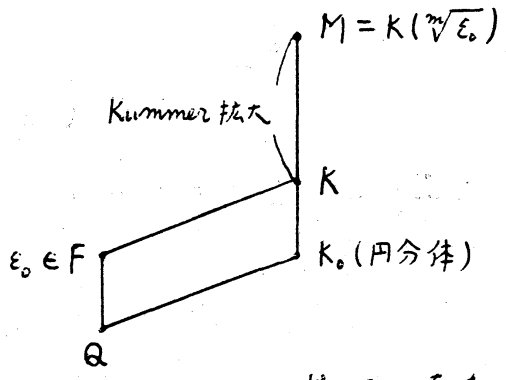
数理解析研究所講究録
41巻 1968年 1-9

Pell方程式の理論の非Abel拡大への応用

東大 教養 黒田 成信

§1. 序

F を定二次体，ε_0 をその基本単数とする．この話の内容は ε_0 の巾根によって生ずる体に於ける有理素数 p の分解を行列群 $\Gamma = GL(2,\mathbb{Z})$ 及びその合同部分群 $\Gamma(p)$ を用いて表わすことにある．即ち自然数 m に対し，適当な円分体 K_0 をとって，$K = F\cdot K_0$ とおき，Kummer体 $K(\sqrt[m]{\varepsilon_0})/K$ に於けるKummer拡大としての分解法則を行列群 Γ の中で表わそうというのである．



我々が対象とする体は左図のような代数的構造をもつ拡大であるが，ε_0 は単数であるから，M/K で分岐しうる素イデアルは m をわる素イデアルに限られる．

後に $(m, 6) = 1$ なる m に対し，M/K が不分岐拡大になる条件を ε_0 の型によって定める．逆に K 上の不分岐 Abel 拡大のうち，どの程度がこのようにして得られるのかは Scholz [3] 及び Leopoldt [2] による所謂 Spiegelungssatz によってある程度のことが分るのである．

今，$m = 3$，$F = Q(\sqrt{3 \cdot 23})$，$K_0 = Q(\sqrt{-3})$ とする．そのとき実は上記 M は $E = Q(\sqrt{-23})$ 上の絶対類体 L を含み，

有理素数 $p (\neq 3, 23)$ が L で完全分解 $\Longleftrightarrow$ $\left(\frac{-23}{p}\right) = 1$ かつ行列 $\begin{pmatrix} 23 & 15 \\ 3 & 2 \end{pmatrix} (\in \Gamma)$ が $\Gamma/\Gamma(p)$ の元として 3 乗

というようなことが，この話の具体的実例である．但し

(0) $$\Gamma(p) = \left\{ A \in \Gamma \mid A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p} \right\}$$

とおいた．$\left(\frac{*}{*}\right)$ は Legendre の記号である．

以下の我々の主張の証明に関しては，一つ一つの議論はごく簡単であるから，今は唯その概略を記すにとどめる．

§2. 記号．

Q 有理数体，　　Z 有理整数環，

$l^\nu\ (\nu \geq 1)$　　固定された素数 l の ν 乗．

$F = Q(\sqrt{d})$　　判別式 d の実二次体，

N　　F から Q へのノルム，

$\varepsilon_0\ (>1)$　　F の基本単数，

ζ ：
- 1の原始 l^ν 乗根，　$l \neq 2$ 又は $N(\varepsilon_0) = 1$ のとき
- 1の原始 $2^{\nu+1}$ 乗根，　$l = 2$ でしかも $N(\varepsilon_0) = -1$ のとき

$K = F \cdot K_0$，但し　$K_0 = Q(\zeta)$，

$M = K(\sqrt[l^\nu]{\varepsilon_0})$．

更に

$$\Gamma = GL(2, \mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid \alpha\delta - \beta\gamma = \pm 1,\ \alpha, \beta, \gamma, \delta \in \mathbb{Z} \right\},$$

$\Gamma(p)$ は上記 (0) の通りとする．　又 $f_{K/Q}(p)$ によって Abel 拡大 K に於ける p の次数を表わす．

ζ のきめ方により M/Q は Galois 拡大である．　それが Abel 拡大になるのは $l = 2$，$\nu = 1$，しかも $N(\varepsilon_0) = 1$ の場合に限られる．　その場合には Galois 群は $(2, 2)$ 型の Abel 群となる (Cf. Furuta [1], §3)．

我々の目的のためには，§1 で述べた m が素数巾の場合だけを考察すれば充分であることは言うまでもない．

§3.

θ を判別式 d の実二次無理数，即ち

(1)
$$a\theta^2 + b\theta + c = 0, \quad a>0, \quad a, b, c \in \mathbb{Z},$$
$$d = b^2 - 4ac$$

とする．θ' を θ の共役とし，$\theta > \theta'$ と規格化されているものとする．更に $\theta > 1$, $0 > \theta' > -1$ のとき，θ は簡約されていると言われる．以下 θ としては，modular 変換による同値類の代表だけを考察しても一般性が失なわれない．従ってともかく θ としては簡約されたものだけを対象とすれば充分なのである．そのとき，(1) の a, b, c の決定法は古典的に周知である．

「命題1．θ $(\theta > \theta')$ を方程式 (1) を充す判別式 d の実二次無理数とする．行列 $A_0 = \begin{pmatrix} \alpha_0 & \beta_0 \\ \gamma_0 & \delta_0 \end{pmatrix}$ を

$$\begin{cases} \varepsilon_0 = \gamma_0\theta + \delta_0, \\ \theta = \dfrac{\alpha_0\theta + \beta_0}{\gamma_0\theta + \delta_0}, \quad \alpha_0, \beta_0, \gamma_0, \delta_0 \in \mathbb{Z} \end{cases}$$

によって定める．（そのとき実は $A_0 \in \Gamma$ である）．p を l と d に素な有理素数とし，更に

$$c(p) = (p^{f_{H/Q}(p)} - 1)/l^{\nu}$$

とおく．$l^{\nu(p)}$ を

$$A_0^{c(p)}\ell^{\nu(p)} \in \Gamma(p)$$

が成り立つ最小の ℓ の巾とする．そのとき p は M に於て絶対次数 $f_{K/\mathbb{Q}}(p)\cdot\ell^{\nu(p)}$ 次の素イデアルの積に分解する．」

今 F の単数 $\varepsilon = \dfrac{t+u\sqrt{a}}{2}$，$t, u \in \mathbb{Z}$ に対し，(1) の a, b, c を用いて

$$A(\varepsilon) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \dfrac{t-bu}{2} & -cu \\ au & \dfrac{t+bu}{2} \end{pmatrix}.$$

とおくと，対応 $\varepsilon \longrightarrow A(\varepsilon)$ は F の単数群の Γ に於ける忠実な表現を与え，更に

(2) $$\varepsilon = \gamma\theta + \delta$$

(3) $$\theta = \frac{\alpha\theta+\beta}{\gamma\theta+\delta}$$

が成たされている(高木[4], 第三章)．命題 1 に於ける A_0 は上記の対応で ε_0 に対応する $A(\varepsilon_0)$ を (2) 及び (3) によって定めたものである．

(1) に於ける a, b, c の選択によって，判別式 d の二次形式の類が一つ定まる．それに対応して上述の単数群の表現の共役類が定まるのである．

単数群の表現 $A(\varepsilon)$ は F の $\mathbb{Q}$ 上の Algebra としての表現の縮少である。性質 (2) は F に対して一般である。

命題1は次の補題，及び巾剰余に関する所謂 Euler の判定条件，Kummer 拡大の分解法則から得られる。

「補題。 p を d に素な素数とする。 $\mathfrak{p}$ を F に於ける p の素因子，ε は F のノルム $+1$ の単数とする。そのとき

$$\varepsilon \equiv 1 \pmod{\mathfrak{p}} \iff A(\varepsilon) \in \Gamma(p).」$$

この補題の証明は $A(\varepsilon)$ の表示を用いて出来る。その際 $p=2$ であれば，上記補題に於て ε に対する符号条件は不要であることが分る。命題1の証明の細部に於てはこの種の注意も必要となろう。

さて，Γ の元 A が $\Gamma/\Gamma(p)$ に於て m 乗であるとき A を Γ に於て $\bmod p$ の m 巾剰余と呼ぶことにしよう。$\Gamma/\Gamma(p)$ のよく知られた構造と命題1とから次の定理をうる。

「定理。 $\ell \neq 2$ とする。 $\mathfrak{p}$ を ℓ と d に素な F の素イデアルとする。更に $\mathfrak{p}$ は K/F で完全分解しているとする。そのとき

$\mathfrak{p}$ が M/F で完全分解 $\iff$ A_0 が $\bmod p$ で ℓ^ν 巾剰余。」

$l=2$ のときに，命題1を上記定理の型に表わすためには，$p+1$ 及び $p-1$ に入る2の巾に対する考察が必要となる．

§4.

l を奇の素数とする．K_0 は1の l 乗根の体とする．即ち $\nu=1$．F，K は §2 の通り．F の数 α は $K(\sqrt[l]{\alpha})/K$ が不分岐拡大のとき，l-primär，又 l をわる素点はすべて $K(\sqrt[l]{\alpha})/K$ で完全分解するとき l-hyperprimär と呼ばれる．以下それを単に primär，hyperprimär と略称する．

「命題2．$\varepsilon_0=\dfrac{t+u\sqrt{d}}{2}$，$t,\ u\in\mathbb{Z}$ を F の基本単数とする．今 F の判別式 d は l でわれているものとする．

i)．$l>3$；　$u\equiv 0 \pmod{l} \iff \varepsilon_0$ が hyperprimär

$\iff \varepsilon_0$ が primär．

ii)．$l=3$；　$u\equiv 0 \pmod 3 \implies \varepsilon_0$ が primär，

$u\equiv 0 \pmod 3 \impliedby \varepsilon_0$ が hyperprimär．」

この命題の証明には，Kummer 拡大に関するごく基本的事実の他に，

(4)　$$\varepsilon_0^{\,2}=\frac{(t^2+du^2)+2tu\sqrt{d}}{4}$$

(5) $$N(\varepsilon_0^{-1}) = \frac{(t^2+du^2)^2 - 4t^2u^2d}{16} = 1$$

に於て (4) の最初の項の平方が (5) の最初の項になっていることと, l/d 等に注意して簡単な計算を行なえばよい。

§1 に述べた例についていえば, $F = Q(\sqrt{3\cdot 23})$, $\theta = \frac{7+\sqrt{69}}{2}$ から A_0 をめると $A_0 = \begin{pmatrix} 23 & 15 \\ 3 & 2 \end{pmatrix}$, F の基本単数 $\varepsilon_0 = \frac{t+u\sqrt{69}}{2} = \frac{25+3\sqrt{69}}{2}$ に於て $u \equiv 0 \pmod 3$. 従って M/K は不分岐拡大となる (§2 の記号で, $l=3$, $\nu=1$ $F = Q(\sqrt{3\cdot 23})$ とおいたのである). M/F, M/K_0 の Galois 群が三文字の対称群と同型であること, 更に $M \supset E = Q(\sqrt{-23})$ であり, M/E の Galois 群が 6 次の環状群であることは容易に分る。従って M/E は E 上 3 次の不分岐 Abel 拡大 L を含むことが帰結される。従って $Q(\sqrt{-23})$ の類数は 3 の倍数でなければならないが, それは丁度 3 に等しいから L は E の絶対類体となっており, §3 の定理の分解法則を今の M/Q にあてはめたものから, §1 に述べた形の L ($L \subset M$) に於ける分解法則が得られるのである。

文　献

[1]. Y. Furuta: Norm of units of quadratic fields, Journ. Math. Soc. Japan, 11(1959), 139-145.

[2]. H. W. Leopoldt: Zur Struktur der l-Klassengruppe galoisscher Zahlkörper, Journ. reine angew. Math. 199 (1958), 165-174.

[3]. A. Scholz: Über die Klassenzahlen quadratischer Körper zueinander, Journ. reine angew. Math. 166(1931), 201-203.

[4]. 高木貞治: 初等整数論講義, 東京(1931).